550,216

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年10 月20 日 (20.10.2005)

PCT

(10) 国際公開番号
WO 2005/099170 A1

(51) 国際特許分類[7]: H04L 9/36

(21) 国際出願番号: PCT/JP2005/006624

(22) 国際出願日: 2005 年4 月4 日 (04.04.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-111347 2004 年4 月5 日 (05.04.2004) JP
特願2004-119225 2004 年4 月14 日 (14.04.2004) JP

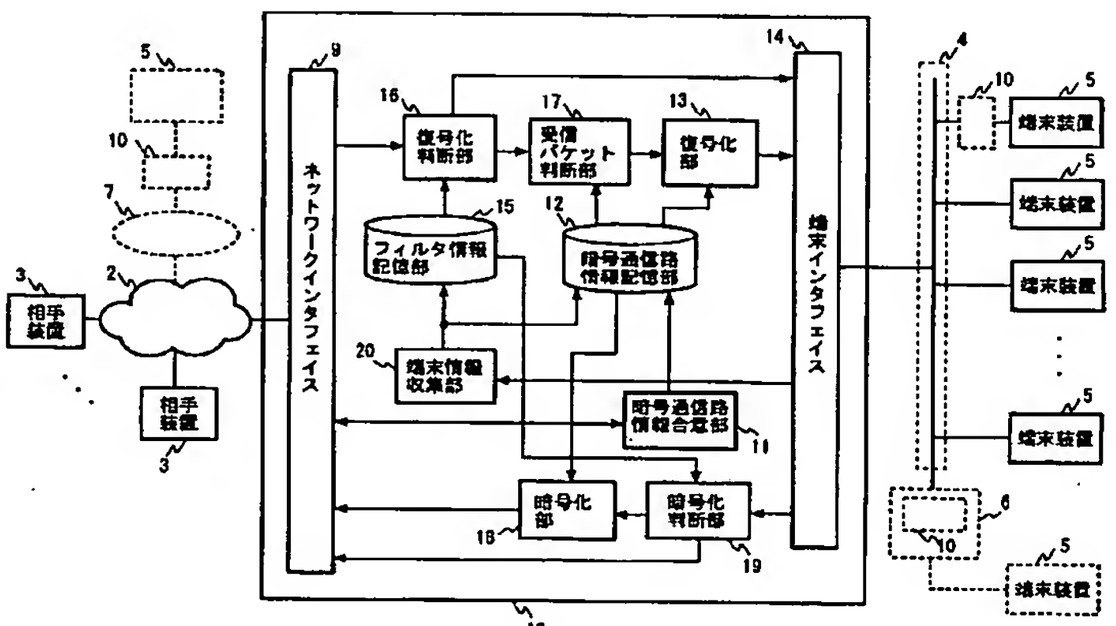
(71) 出願人 (米国を除く全ての指定国について): 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町二丁目３番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 唐澤 圭 (KARASAWA, Kei) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号ＮＴＴ知的財産センタ内 Tokyo (JP). 松浦 克智 (MATSUURA, Katsunori) [JP/JP]; 〒1808585 東京都武蔵野市緑町三丁目９番１１号ＮＴＴ知的財産センタ内 Tokyo (JP).

[続葉有]

(54) Title: PACKET ENCRYPTION SUBSTITUTING DEVICE, METHOD THEREOF, AND PROGRAM RECORDING MEDIUM

(54) 発明の名称: パケット暗号処理代理装置



3 PARTNER DEVICE
9 NETWORK INTERFACE
16 DECRYPTION JUDGMENT UNIT
17 RECEPTION PACKET JUDGMENT UNIT
13 DECRYPTION UNIT
15 FILTER INFORMATION STORAGE UNIT
12 ENCRYPTED COMMUNICATION PATH INFORMATION STORAGE UNIT
20 TERMINAL INFORMATION COLLECTION UNIT
11 ENCRYPTED COMMUNICATION PATH INFORMATION AGREEMENT UNIT
18 ENCRYPTION UNIT
19 ENCRYPTION JUDGMENT UNIT
14 TERMINAL INTERFACE
5 TERMINAL DEVICE

(57) Abstract: When a packet is received from a partner device (3) connected to the Internet (2), a filter information storage unit (15) is referenced according to the transmission source and transmission destination IP address/port number in the packet and the protocol and a decryption judgment unit (16) judges whether to perform decryption or bypass. If it is judged to perform decryption, the reception packet is decrypted according to encrypted communication path information agreed in advance by the partner device (3) and a terminal device (5) not having the IPSec function and the reception packet is sent to the terminal device (5) from the encryption path information storage unit (12). The encrypted communication path information is used to establish a packet communication path based on the IPSec between the partner device (3) and the terminal device (5) and includes an identification number, protocol information on the encryption process or signature process, encryption algorithm, key information, IP address/port number, and the like. The partner can use the transport mode.

(57) 要約: インターネット２に接続された相手装置３からパケットが受信されると、そのパケット中の送信元及び送信先のＩＰアドレス・ポート番号、プロトコルにより、フィルタ情報記憶部１５を参照して、復号化するかバ

[続葉有]

WO 2005/099170 A1

(74) 代理人: 草野 卓 (KUSANO, Takashi); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル４階 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

イパスするかを復号化判断部１６で判断し、復号化と判断されると、暗号通信路情報記憶部１２から、相手装置３とIPSec機能を持たない端末装置５とで予め合意された暗号通信路情報に基づいて受信パケットを復号化して端末装置５へ送る。暗号通信路情報は相手装置３と端末装置５の間にIPSecに準拠したパケット通信路を確立するために用い、識別番号、暗号化処理か署名処理かのプロトコル情報、暗号アルゴリズムや鍵情報、ＩＰアドレス・ポート番号などである。相手はトランスポートモードを使用できる。

明 細 書

パケット暗号処理代理装置

技術分野

[0001] この発明は、端末装置とインターネットとの間に接続され、インターネットに接続された相手装置と前記端末装置間のパケット通信において、暗号処理されたパケットに対し前記端末装置に代わって暗号処理を代行可能なパケット暗号処理代理装置、その方法及びプログラムの記録媒体に関するものである。

背景技術

[0002] 従来、インターネット等のネットワークを介して暗号通信を行なうための規格として、インターネットの標準化組織であるIETF(Internet Engineering Task Force)により標準化され、フレーム構成、データの暗号化及び復号化や改ざんチェックなどの規定に準拠したIPSec(Security Architecture for Internet Protocol)がRFC(Request for Comments)2401(以下非特許文献1と呼ぶ)に示されている。その他の暗号通信プロトコルの規格として、SSL(Secure Sockets Layer)やTLS(Transport Layer Security)等がある。これらの規格は、事前に暗号及び復号、署名及び検証するための鍵、暗号及び復号化アルゴリズム、署名及び検証アルゴリズム、及びプロトコル等のSA(Security Association)情報を合意しておく。このSA情報の合意は、鍵交換プロトコルであるIKE(Internet Key Exchange)やハンドシェーク(Handshake)プロトコルに準拠して行われる。

[0003] IPSec機能は、必要に応じて端末装置に実装される。IPSec機能はその他に、インターネットを利用した仮想的に構築する独自ネットワークであり、標準プロトコルとしてIPSecを規定するVPN(Virtual Private Network)におけるパケット暗号処理代理装置に実装される。つまり例えばインターネットとLAN(Local Area Network)を接続するゲートウェイ内にIPSec機能が設けられ、ゲートウェイがLANに接続された各端末装置(以下、内部端末装置と呼ぶ)に代ってパケットに対する暗号処理を行う。つまりインターネットに接続された端末装置(以下、外部装置または相手装置と呼ぶ)は、LANに接続された内部端末装置に対し、データを暗号化しないで通信を行う場合はそ

のパケットにそのLANの内部端末装置のIPアドレス等を設定すればよいが、データを暗号化する場合はLANの内部端末装置のIPアドレス等を設定し、これとデータを含むパケットを生成し、そのパケット全体に対して所定の暗号化を行い、その暗号化されたパケットに、パケット暗号処理代理装置を兼ねるゲートウェイのIPアドレスなどを設定したパケットを生成し、そのパケットを送信する。このパケットを受信したゲートウェイはそのパケットを復号化し、復号されたパケットを、そのヘッダが示すIPアドレスに基づきLANの内部端末装置に送信する。従ってこの場合のゲートウェイはパケット暗号処理代理装置を兼ねているといえる(第1従来技術という)。

[0004] このようなパケット暗号処理代理装置としては、例えば、アクセスが制限された閉鎖型ネットワークに接続され、閉鎖型ネットワークとゲートウェイを経由して接続された開放型ネットワークに接続された端末装置(外部装置と対応するもの)との暗号通信を閉鎖型ネットワークに接続された内部端末装置に代行して行うものが例えば日本国特許出願公開2003-304227号公報(以下特許文献1と呼ぶ)に示されている(以下、第2従来技術と呼ぶ)。

図8を参照してこの特許文献1に示す従来のパケット暗号処理代理装置を説明する。図8に示すように閉鎖型ネットワークであるホームネットワーク104に接続された家庭内ノード(内部端末装置)122と、開放型ネットワークであるインターネット102に接続された外部ノード(外部装置)106との間で、インターネット102とホームネットワーク104間に介在されたホームゲートウェイ108を介して暗号通信を行う。家庭内ノード(この例では電子レンジ)122は、暗号化と復号化の処理を行うのに充分なデータ処理性能を備えていない。よってホームネットワーク104にパケット暗号処理代理装置として暗号代行家庭内サーバ120がホームネットワーク104に接続され、家庭内ノード122と外部ノード106と暗号化通信を行うためのデータ暗号化と復号化の処理を、家庭内サーバ120が家庭内ノード122に代わって行う。

[0005] 外部ノード106が暗号通信の起動を行う場合には外部ノード106は、インターネット102、ホームゲートウェイ108、ホームネットワーク104を経由して暗号通信要求パケットを、家庭内ノードの電子レンジ122に送る(S21)。この暗号通信要求パケット内のデータは、外部ノード106が家庭内ノードである電子レンジ122と暗号通信を確立す

るために必要なデータであり、電子レンジ122に問い合わせるデータである。電子レンジ122は、このような暗号通信要求パケットを受信したならば、外部ノード106に対して、逆の経路で暗号通信承諾パケットを送信する(S22)。この暗号通信承諾パケット内のデータには暗号通信を承諾すると共に同じホームネットワーク104に接続された家庭内サーバ120のネットワークアドレスが含まれている。

[0006] 暗号通信承諾パケットを受信した外部ノード106は、指定された暗号通信代行サーバである家庭内サーバ120に対して、インターネット102、ホームゲートウェイ108、ホームネットワーク104を経由して、暗号通信代行要求パケットを送信する(S23)。暗号通信代行要求パケットを受信した家庭内サーバ120は、暗号通信代行承諾パケットを、その外部ノード106に送信する(S24)。これによって外部ノード106は、家庭内ノード122との暗号通信を代行することを確認する。外部ノード106は、家庭内サーバ120が、家庭内ノード122との暗号通信を代行して行うことを確認した後、或いは、これらの確認の全部又は一部を省略して、予め定められた所定の手順に従って暗号化されたデータパケットを家庭内サーバ120に送信する(S25)。所定の手順に従って暗号化されたデータパケットを受信した家庭内サーバ120は、その受信したデータパケットを復号化し、ホームネットワーク104を経由して、本来の通信相手であるべき家庭内ノード122(電子レンジ)にその復号化されたデータパケットを送信する(S26)。これによって、家庭内ノード122(電子レンジ)は、高度な暗号化、復号化のための処理能力をもたなくても、本来の目的である外部ノード106との暗号通信を実現することができる。

[0007] IPSecにおける鍵交換プロトコルを実行するには、SA情報を互いに合意する両者装置間で複数回の通信を行い、しかも計算処理量がかなり多く、これら装置に対し大きな負荷となる。従って、例えば家庭内の暗号処理通信機能を備える電子機器など小規模の端末装置にSA情報合意機能を設けるとハードウェア及びソフトウェア規模が大きくなり、大形化になりかつ価格も高くなる。このような点から、端末装置に暗号処理機能は設けるが、SA情報の合意－処理を端末装置に代って鍵支援代理装置で行うことが例えば日本国特許出願公開2003-179592号公報(以下、特許文献2と呼ぶ)に提案されている。この特許文献2に示す鍵交換代理技術によれば、ネットワーク

に接続され、暗号処理機能は有するが鍵交換機能を備えない端末装置が、ネットワークに接続され、鍵交換機能を備えた通信相手側端末装置とパケット暗号通信を行う場合、端末装置32はまず通信相手側端末装置との暗号通信信号に用いる共通鍵の交換を、ネットワークに接続された鍵交換代行サーバに要求し、鍵交換代行サーバはその要求に基づき、端末装置に代って通信相手側端末装置と鍵交換処理を行い、合意した共通鍵を端末装置に設定する。その後、端末装置はその合意した共通鍵を用いて通信相手側端末装置とパケット暗号通信を行う。

[0008] このような鍵交換代理処理をゲートウェイで行わせることが日本国特許出願公開2003-289299号公報(以下、特許文献3と呼ぶ)に示されている。

第1従来技術ではインターネットに接続された外部装置は、LANの端末装置に対して、暗号化することなくパケットを送信する場合は、単にそのLANの端末装置のIPアドレスなどを設定すればよいが、暗号化してパケットを送信する場合は、パケットを暗号化し、その暗号化されたパケットをデータとし、これに対してゲートウェイ(パケット暗号処理代理装置)のIPアドレスなどを設定してパケットを送信する必要がある。つまり暗号化されないパケットの終端はLANの端末装置であり、暗号化パケットの終端はゲートウェイである。このように暗号通信を行う場合はゲートウェイのIPアドレスなども設定する必要があり、同一端末装置に対する通信にそのIPアドレスなどの他にゲートウェイのIPアドレスなどを設定するという繁雑さがあった。

[0009] 第2従来技術では、暗号化パケットの終端がパケット暗号処理代理装置にあたる家庭内サーバ120であり、パケットの送信先の終端が端末装置(電子レンジ)122であるため、家庭内サーバ120を導入した場合には、インターネットに接続された相手装置は暗号通信にするか否かによりIPアドレス等の設定情報を変更する必要があり、第1従来技術と同様に通信相手(相手装置を操作する人)に設定の手間をかけてしまうといった問題があった。また、前述したようなこの第2従来技術では、暗号通信を行うにはまず電子レンジ122に対し暗号通信要求を行って代行サーバの指定を受け、改めてサーバ120に対し暗号通信代行要求とその承諾を受けて暗号化パケットを送るという多くの手間がかかるという問題もあった。

特許文献1:日本国特許出願公開2003-304227号公報

特許文献2：日本国特許出願公開2003-179592号公報

特許文献3：日本国特許出願公開2003-289299号公報

非特許文献1：RFC（Request for Comments）2401

発明の開示

発明が解決しようとする課題

[0010] この発明は、これらの問題を解決するためになされたものであり、通信相手に設定の手間をかけずに、暗号処理機能が実装されていない端末装置に対して暗号処理を代行することができるパケット暗号処理代理装置、その方法及びプログラムを記録した記録媒体を提供することを目的とするものである。

課題を解決するための手段

[0011] この発明によるパケット暗号処理代理装置は、インターネットと端末装置との間に接続され、暗号通信路情報記憶部及び暗号処理部を備え、暗号通信路情報記憶部には、インターネットに接続された相手装置と上記端末装置との間のパケット通信における少なくともインターネット上のパケット通信に対し、暗号通信路確立に用いる暗号通信路情報が記憶され、暗号処理部では受信されたパケットに対して、暗号通信路情報記憶部に記憶されている暗号通信路情報に基づいて暗号処理が行われる。

発明の効果

[0012] 以上説明したように、この発明のパケット暗号処理装置によれば、ネットワーク端末装置との間に接続されているから、例えばインターネットに接続された相手装置では暗号処理機能を備えない端末装置のIPアドレスなどを設定すれば暗号処理されたパケットに対する暗号処理、例えば復号が行われるため、つまり相手装置はトランスモードを探ることができ、端末装置のIPアドレスなどとパケット暗号処理代理装置IPアドレスなどとの設定を行う必要がなく、相手装置の利用者に設定の手間をかけない。また端末装置との通信により暗号処理代行サーバのIPアドレスなどの入手の後、そのサーバのIPアドレスなどを設定して暗号処理されたパケットを暗号処理代行サーバへ送信するなどの煩雑さもない。

図面の簡単な説明

[0013] [図1]この発明によるパケット暗号処理代理装置の第1実施例のシステム構成例を示すブロック図。

[図2]図2Aは図1中の暗号通信路情報記憶部12に記憶されているSA情報の例を示す図、図2Bは図1中のフィルタ情報記憶部15に記憶されているフィルタ情報の例を示す図、図2Cはパケットの構成例を示す図。

[図3]この発明の第1実施例による相手装置から受信したパケットに対する処理手順の例を示すフローチャート。

[図4]この発明の第1実施例による端末装置から受信したパケットに対する処理手順の例を示すフローチャート。

[図5]この発明によるパケット暗号処理代理装置の第2実施例のシステム構成例を示すブロック図。

[図6]第2実施例による相手装置から受信したパケットに対する暗号通信路情報合意手順の例を示すフローチャート。

[図7]第2実施例による端末装置から受信したパケットに対する暗号通信路情報合意手順の例を示すフローチャート。

[図8]従来のパケット暗号処理代行サーバを含むシステム及び代行暗号処理の通信手順を示す図。

発明を実施するための最良の形態

[0014] 以下、この発明の実施例について、図面を参照して説明する。

第1実施例

図1は、この発明の第1の実施例に係るパケット暗号処理代理装置10を含むシステムの構成例を示すブロック図である。以下の説明ではパケット暗号処理をIPSecに基づいて行う場合を例とし、暗号処理として暗号化処理及び復号化処理を例とする。

パケット暗号処理代理装置10はインターネット2に接続され、インターネット2には外部装置3が接続される。パケット暗号処理代理装置10はパーソナルコンピュータや通信機能を備え、家庭内電気製品等の内部端末装置5にLAN4を介して接続されている。内部端末装置5としては、IPSec機能が実装されているもの、いないもの、暗号処理機能は実装されているが鍵交換機能(暗号通信路情報合意機能)が実装されて

ないものなどが混在している。この実施例においては、外部装置3は、IPSec機能が実装されたものとする。つまりこの実施例ではパケット暗号処理代理装置10はインターネット2とLAN4とを接続するゲートウェイと兼用されている。

[0015] パケット暗号処理代理装置10は、ネットワーク2を介して接続された外部装置3と通信を行うネットワークインタフェイス9と、インターネット2上で安全な通信路を確立するために必要な暗号通信路情報を相手装置3と端末装置5との間で合意するための暗号通信路情報合意部11、合意された暗号通信路情報を記憶する暗号通信路情報記憶部12、IPSecに準拠して暗号化されたパケットを復号化する復号化部13、端末装置5などとの通信を行う端末インタフェイス14とを備える。

暗号通信路情報はIPSecに準拠したものであり、本来の通信に先立ち相手装置3と端末装置5との間で双方が通信可能な手順の確認のネゴシエーション、つまり合意が暗号通信路情報合意部11により行われ、その結果の暗号通信路情報が暗号通信路情報記憶部12に記憶される。

[0016] 暗号通信路情報記憶部12は、例えば不揮発性の記憶媒体によって構成される。暗号通信路情報(以下、単に「SA(Security Association)情報」という)は非特許文献1で規定されたものであり、例えば図2Aに示すように、接続要求もとの端末装置のIPアドレスに対応して(1) SA情報を識別するための32ビットの整数値で割り当てられて各パケット中に挿入され、パケット内の通信内容を示す識別番号SPI(Security Parameter Index)、(2) 通信データ完全性を保証して転送し、またその検証を行うためのプロトコルであるAH(Authentication Header)及び通信データを秘匿して転送し、またその秘匿解除するためのプロトコルであるESP(Encapsulating Security Payload)の何れかのプロトコルの情報を表すセキュリティプロトコル情報、(3) 暗号化や認証でそれぞれ使用される暗号アルゴリズムや暗号鍵情報、(4) 受信したパケットをIPヘッダを含めて暗号化して受信先へ転送するモードであるトンネルモード及び、受信したパケット中のデータを暗号化しそれにIPヘッダを付加し、受信先に送るモードであるトランスポートモードの何れかのモードを表すモード情報、(5) 相手IPアドレス及びポート番号よりなる識別子、及び(6) SA情報を変化させる時期などを示すSA情報の存続時間等が含まれる。なお、ポート番号はインターネットで標準化されたサ

ービスプロトコルに割り当てられた番号である。

[0017] この実施例ではモード情報はトランスポートモードとされるが、例えばIPSec機能を備えない端末装置の他にIPSec機能を備えた端末装置が混在しているネットワークとインターネットとの間にこの発明によるパケット暗号処理代理装置10が設けられる場合はモード情報としてはトンネルモードとされたりトランスポートモードにされたりする。またこの実施例ではセキュリティプロトコル情報としてはESPが用いられるが、データが改ざんできないようにするAHプロトコル、具体的には例えばディジタル署名及びその検証のプロトコルを用いてもよい。

[0018] SA情報の各パラメータは、IKE(Internet Key Exchange)等の鍵交換プロトコルによって通信相手との間で合意されるものであり、暗号通信路情報合意部11は、端末装置5に代わってSA情報の各パラメータを相手装置3と合意し、合意したパラメータが反映されたSA情報を暗号通信路情報記憶部12に格納する。

復号化部13は、暗号通信路情報記憶部12に記憶されたSA情報に含まれる暗号アルゴリズムや暗号鍵情報に基づいて、相手装置3によってIPSecに準拠して暗号化されて端末装置5に向けて送信されたパケットをパケットの送信元と送信先を変えずに復号化する。

[0019] 更に、この実施例ではパケット暗号処理代理装置10は、送信元識別情報、送信先識別情報、及びパケット伝送プロトコル情報に対応して、パケットの処理を表す指示情報をフィルタ情報として記憶するフィルタ情報記憶部15と、相手装置3によって送信されたパケットを復号化部13によって復号化するか否かをフィルタ情報に基づいて判断する復号化判断部16を備えている。

復号化判断部16は、フィルタ情報記憶部15に予めシステムの管理者により各端末装置に対応して記憶されているフィルタ情報を参照し、相手装置3によって端末装置5に向けて送信されたパケットを復号化するか(暗号処理)、端末装置5にそのまま端末インタフェイス14を介して送信するか(バイパス)、パケットを廃棄するか、を判断し、判断結果に応じてパケットの処理を決定する。バイパスするのは、(1) 端末装置にIPSec機能が備えられてない場合か、(2) 端末装置に暗号処理機能が備えられているが、鍵交換機能が備えられてない場合か、(3) データが暗号処理を必要としない場

合かである。

[0020] 図2Bは、フィルタ情報の例を示した表である。図2Bにおいて、1列目は、パケットの送信元を識別するための送信元識別情報中の送信元のIPアドレスを表し、2列目はパケットの送信先を識別するための送信先識別情報を構成する送信先のIPアドレス、3列目はパケットを伝送するための通信手順を表すプロトコル情報、4列目は送信元識別情報中の送信元のポート番号、5列目は送信先識別情報中の送信先のポート番号、及び6列目はパケットをどのように処理するかを表す処理指示情報を表している。

前述したように復号化判断部16は、受信したパケット中の処理指示情報以外のフィルタ情報によりフィルタ情報記憶部15にあらかじめ記憶されているフィルタ情報を参照し、その処理指示情報に応じて端末装置5に向けて送信されたパケットを復号化するか、そのまま端末インタフェイス14を介して送信するか、この例では更に廃棄するか、を判断し、判断結果に応じてパケットの処理を決定する。

[0021] 図2B中の1行目のフィルタ情報は、IPSec機能を有してない端末装置に対する情報であり、IPアドレスがIPv4によって書かれており、送信元のIPアドレスが10.0.0.1/32(全32ビット指定)、送信先のIPアドレスが10.0.0.*/24(上位24ビットが指定、下位8ビットが0～255の任意の値)及び、プロトコル情報が信頼性を保証したコネクション形プロトコルであるtcp(Transmission Control Protocol)の場合には、送信元ポート番号及び送信先ポート番号が何番であっても(any)、処理指示情報は相手装置3によって送信されたパケットを暗号処理する。

[0022] 2行目のフィルタ情報は各種暗号処理規定に準拠したプロトコルIPSecの機能を有する端末装置5に対するフィルタ情報の例であり、送信元IPアドレスが10.0.0.2/32、送信先IPアドレスが10.0.1.*/24の暗号処理されたパケットをそのまま端末装置5にバイパスすることを表している。

3行目のフィルタ情報は、IPアドレスがIPv6によって書かれており、送信元のIPアドレスが2001::1、送信先のIPアドレスが2001::2、プロトコル情報が、画像や音声の配信データの場合のようなパケットの紛失を許容するコネクションレス形プロトコルudp(User datagram protocol)であり、送信元のポート番号と送信先のポート番号とが137

の場合には、処理指示情報は相手装置3によって送信された暗号処理されてないパケットを端末装置5にそのまま端末インタフェイス14を介してバイパス送信する。

[0023] また、4行目のフィルタ情報は、送信元のIPアドレスが2001::1/128、送信先のIPアドレスが2001::2/128、プロトコル情報がIP端末同士をコントロールするプロトコルであるicmp(Internet Control Message Protocol)、及び、送信元のポート番号が135の場合には、処理指示情報は相手装置3によって送信されたパケットを廃棄する。

なおこれらのフィルタ情報は例示であって、その識別情報やプロトコル情報と処理指示情報との間に関連はない。

各パケットは、例えば図2Cに示すように、送信元(SRC)IPアドレスと、送信先(DST)IPアドレスと、ESPヘッダまたはAHヘッダと呼ばれる拡張ヘッダSPI+ICVと、プロトコルと、送信元ポート番号と、送信先ポート番号とを含むヘッダ情報部HDを有している。そのヘッダ情報部HDの後にデータ部DAが付加されている。拡張ヘッダSPI+ICVが付加されているか否かにより、データ部DAがIPSecに準拠した暗号処理されているか否かが表される。

[0024] 復号化判断部16は受信したパケット中のフィルタ情報に基づきフィルタ情報記憶部15を参照したらその処理指示情報は復号化であったが、その受信されたパケットのヘッダ情報部HDを参照し、拡張ヘッダが付加されているか否かを判定した結果、付加されてないと判定した場合、すなわち、そのパケットがIPSecに準拠して暗号化されていないと判断されると、このパケットを廃棄するあるいは端末装置5へそのままバイパスしてもよい。

パケット暗号処理代理装置10には、ARP(Address Resolution Protocol、アドレス解決プロトコル)やNDP(Neighbor Discovery Protocol 、近隣発見プロトコル)などの情報収集プロトコルや、UPnP(Universal Plug and Play)などの相互接続機能をもつ端末情報収集部20が設けられており、パケット暗号処理代理装置10に接続されている端末装置5のIPアドレスやサービス等の機器情報を収集し、収集した機器情報に基づいてIPアドレス、ポート番号、プロトコルの種別などの情報を含む図2Bに示すようなフィルタ情報を生成してフィルタ情報記憶部15に記憶する。フィルタ情報中の処理指示はシステム管理者が入力してもよい。

[0025] 端末装置5が外された場合など、システム構成に変更があった場合に、暗号通信路情報及びフィルタ情報のうち少なくとも一方の一部またはすべてをシステム管理者が更新、削除できるようにしてもよい。

この第1実施例では、パケット暗号処理代理装置10は復号化判断部16が復号化と判断した場合に、復号化処理に先立って相手装置3によって送信されたパケットが正当なものであるか否かを判断する受信パケット判断部17がさらに備えられている。受信パケット判断部17によるパケットの正当性の判断は、IPSecに準拠して暗号化されたパケットに含まれる完全性チェック値やIPSecの規定されているパケットに付随しているシーケンス番号等に基づいて行われる。なお、完全性チェック値(Integrity Check Value、ICV)は、認証アルゴリズムによって決定されるアルゴリズムによって算出される。復号化判断部16によりフィルタ情報を参照して受信パケットに対する処理が復号化と判断された場合でも、パケット判断部17がパケットのヘッダ情報からパケットが暗号処理されてないと判断した場合は復号化部13でパケットの復号化処理を行わず、そのまま端末装置5に送出してもよい。

[0026] 更にこの実施例では、パケット暗号処理代理装置10は、暗号通信路情報記憶部12に記憶されたSA情報に基づいて、端末装置5によって送信されたパケットをIPSecに準拠して暗号化する暗号化部18と、フィルタ情報記憶部15に記憶されたフィルタ情報に基づいて、端末装置5によって送信されたパケットを暗号化部18によって暗号化するか否かを判断する暗号化判断部19とが備えられている。

暗号化部18は、暗号通信路情報記憶部12に記憶されたSA情報に含まれる暗号アルゴリズムや暗号鍵情報に基づいて、端末装置5によって相手装置3に向けて送信されたパケットをIPSecに準拠してパケットの送信元と送信先を変えることなく暗号化する。

[0027] 暗号化判断部19は、端末装置5から受信したパケット中のフィルタ情報中の送信元IPアドレスによりフィルタ情報記憶部15に記憶されたフィルタ情報を参照し、端末装置5によって送信されたパケットを暗号化して送信するか、相手装置3にそのままネットワークインタフェイス9を介して送信するか、パケットを廃棄するか、を判断し、判断結果に応じてパケットの処理を決定する。なお、暗号化判断部19によって参照される

フィルタ情報は、図2Bを用いて説明した復号化判断部16によって参照されるフィルタ情報と同様であるため、説明を省略する。ただ同一フィルタ情報であっても相手装置3から端末装置5へのパケットと、端末装置5から相手装置3へのパケットとにより前者は復号化するが、後者は暗号化しないなど処理指示情報が異なる場合もあり、個々に決められている。

[0028] フィルタ情報を参照する暗号化判断部19を設けることによって、パケット暗号処理代理装置10は、複数の端末装置が接続された場合に、あらかじめ予定(許可)されていない不正な端末装置を相手装置と接続するのを防ぐことができ、同様にあらかじめ予定(許可)されていない不正な相手装置3との間で暗号通信が行われることを防ぐことができる。

以下に、パケット暗号処理代理装置10の動作を説明する。なお、以下に説明するパケット暗号処理代理装置10の各動作において、暗号通信路情報合意部11によって合意されたパラメータが反映されたSA情報が、暗号通信路情報記憶部12に既に記憶されているものとする。

[0029] 図3は、パケット暗号処理代理装置10による相手装置3からの受信パケットに対する処理を示すフローチャートである。ステップS1でパケットが受信されるとそのパケットが通信路情報(SA情報)の合意(例えば暗号鍵の交換)を要求しているか判定し(ステップS2)、要求していればステップS3で通信路情報の合意を行い、合意された通信路情報を端末IPアドレスに対応して暗号通信路情報記憶部12に書き込んでステップS1に戻り、次のパケットを受信する。

ステップS2で受信パケットが通信路情報の合意を要求していなければ、復号化判断部16が、ネットワークインタフェイス9によって受信したパケット中のフィルタ情報によりフィルタ情報記憶部15に記憶されたフィルタ情報を参照し、受信されたパケットを復号化するか否かが判断され(ステップS4)、復号化すると判断されないと端末装置5にそのまま端末インタフェイス14を介して送信するか否かが判断され(ステップS5)、そのまま送信しないと判断されるとその受信パケットは復号化判断部16により廃棄される(ステップS7)。

[0030] ステップS4でパケットを復号化すると判断された場合には、ネットワークインタフェイ

ス9によって受信されたパケットが正当なものであるか否かが受信パケット判断部17によって判断される(ステップS6)。ネットワークインタフェイス9によって受信されたパケットが正当なものでないと判断された場合には、ネットワークインタフェイス9によって受信されたパケットが受信パケット判断部17によって廃棄される(ステップS7)。

一方、ステップS6でネットワークインタフェイス9によって受信されたパケットが正当なものであると判断された場合には、ネットワークインタフェイス9によって受信されたパケットが暗号通信路情報記憶部12に記憶されたSA情報に基づき復号化部13によって復号化され(ステップS8)、復号化されたパケットが端末インタフェイス14及びLAN4を介して端末装置5に送信され(ステップS9)、ステップS1に戻って次のパケットを受信する。

[0031] ステップS5で、ネットワークインタフェイス9によって受信されたパケットを端末装置5にそのまま端末インタフェイス14を介して送信すると復号化判断部16によって判断された場合には、ネットワークインタフェイス9によって受信されたパケットがそのまま端末インタフェイス14及びLAN4を介して端末装置5に送信される(ステップS9)。

図4は、パケット暗号処理代理装置10が端末装置5から受信したパケットに対して行う処理のフローチャートである。図3の場合と同様に、ステップS11でパケットが受信されるとそのパケットが通信路情報(SA情報)の合意(例えば暗号鍵の交換)を要求しているか判定し(ステップS12)、要求していればステップS3で相手装置3との通信路情報の合意を行い、合意された通信路情報を端末IPアドレスに対応して暗号通信路情報記憶部12に書き込んでステップS11に戻り、次のパケットを受信する。

[0032] ステップS12で受信パケットが通信路情報の合意を要求していなければ、暗号化判断部19により、端末インタフェイス14で受信されたパケットのフィルタ情報に基づきフィルタ情報記憶部15に記憶されたフィルタ情報を参照して、その受信されたパケットを暗号化するか否かが判断され(ステップS14)、暗号化しないと判断されると、相手装置3にそのままネットワークインタフェイス9を介して送信するか否かが判断され(ステップS15)、そのまま送信しないと判断された場合、パケットを廃棄すると判断された場合には、その受信されたパケットが暗号化判断部19によって廃棄される(ステップS18)。

[0033] ステップS14でパケットを暗号化すると判断された場合には、端末インタフェイス14によって受信されたパケットが、暗号通信路情報記憶部12に記憶されたSA情報に基づき暗号化部18によってIPSecに準拠して暗号化され(ステップS16)、その暗号化されたパケットがネットワークインタフェイス9及びインターネット2を介して相手装置3に送信し(ステップS17)、ステップS11に戻って次のパケットを受信する。

ステップS15で端末インタフェイス14によって受信されたパケットを相手装置3にそのままネットワークインタフェイス9を介して送信すると暗号化判断部19によって判断された場合には、端末インタフェイス14によって受信されたパケットがネットワークインタフェイス9及びインターネット2を介して相手装置3に送信される(ステップS17)。

<u>第2実施例</u>

図5はこの発明によるパケット暗号処理代理装置の第2の実施例を示す。この実施例は、図1の実施例における暗号通信路情報合意部11による暗号通信路情報の合意手順を具体的に実施するため、図1のパケット暗号処理代理装置10に、さらにパケット判断部21及び23と鍵情報設定部22とを付加したものである。従って、受信パケットに対する処理は基本的に図3及び4で説明した処理と同じであり、説明を省略する。

[0034] パケット判断部21は外部装置3からの受信パケットが暗号通信路情報の合意を要求しているかを判定し、要求している場合は通信路情報合意部11により外部装置3と暗号通信路情報の合意を行い、合意された暗号通信路情報(SA情報)を暗号通信路情報記憶部12に書き込む。必要があれば、書き込まれた暗号通信路情報中の鍵情報を設定部22により送信先IPアドレスの端末装置5に送信する。パケット判断部23は端末装置5からの受信パケットが通信の開始を要求しているかを判定し、要求している場合は通信路情報合意部11により外部装置3と暗号通信路情報の合意を行い、合意された暗号通信路情報(SA情報)を暗号通信路情報記憶部12に書き込む。必要があれば、書き込まれた暗号通信路情報中の鍵情報を設定部22により送信元IPアドレスの端末装置5に送信する。

[0035] 図6は、相手装置3からの受信パケットに対するパケット暗号処理代理装置10による暗号通信路情報合意処理を示すフローチャートである。図6のステップS2-1～S2-

4は図3におけるステップS2の詳細であり、図6のステップS3-1～S3-4は図3におけるステップS3の詳細である。

ステップS1で相手装置3からパケットが受信されると、ステップS2-1で受信パケットの送信先IPアドレスがフィルタ情報記憶部15に記憶されているかをパケット判断部21により判定し(ステップS2-1)、記憶されてないと判定された場合は受信パケットがパケット判断部21によって廃棄される(ステップS2-2)。一方、パケットの送信先IPアドレスがフィルタ情報記憶部15に記憶されていると判定された場合は、受信パケットが暗号通信路情報合意要求(鍵交換要求)に関するものか否かがパケット判断部21によって判断される(ステップS2-3)。

[0036] ステップS2-3で、受信パケットが暗号通信路情報合意要求に関するものでないと判断された場合は、図3のステップS4に移り、ステップS4～S9により受信パケットの処理を行う。一方、受信パケットが暗号通信路情報合意要求に関するものであると判断された場合には、ステップS2-4でその受信パケットに示されているSA情報識別番号と同一でかつ存続期間が有効なSA情報が既に暗号通信路情報記憶部12に記憶されているかが判断され、記憶されていなければステップS3-1でSA情報が暗号通信路情報合意部11によって相手装置3と暗号通信路情報の合意を行う。

[0037] ステップS3-1で、相手装置3と合意されたSA情報は、ステップS3-2で暗号通信路情報記憶部12に記憶され、ステップS3-3で、フィルタ情報記憶部15に記憶されている送信先IPアドレスの端末装置に関するフィルタ情報を参照して送信先の端末装置が暗号処理機能を備えているか判定する。この判定は、例えば図2Bに示す送信先端末装置に関するフィルタ情報のプロトコルがtcpであり、かつ、処理指示がバイパスとなっている場合にその端末装置は暗号処理機能を備えていると判定する。暗号処理機能を有していると判定した場合は、ステップS3-4でその合意したSA情報中の鍵情報を鍵情報設定部22によって端末インタフェイス14を介して端末装置5に送信し、ステップS1に戻って次のパケットを受信する。

[0038] ステップS3-3で端末装置が暗号処理機能を備えてないと判定した場合は、そのままステップS1に戻って次のパケットを受信する。

ステップS2-4で有効なSA情報が記憶されていると判断されると、ステップS3-3に

移り、前述と同様の処理を行う。なお、端末装置5は鍵情報設定部22により与えられた鍵情報が表す鍵を使って端末装置5と相手装置3との間で伝送されるパケットの暗号化及び復号化を行うが、端末装置5に鍵情報を送らない場合（すなわち端末装置が暗号処理機能を備えてない場合）は、端末装置と相手装置間で伝送されるパケットに対し、パケット暗号処理代理装置10が暗号化、復号化を代行する。

[0039] 図7は、端末装置5からの受信パケットに対するパケット暗号処理代理装置10による暗号通信路合意処理を示すフローチャートである。図7のステップS12-1～S12-4は図3におけるステップS12の詳細であり、図7のステップS13-1～S13-4は図3におけるステップS13の詳細である。図7の処理は図6の処理とほぼ同様である。

ステップS11で端末装置5からパケットが受信されると、ステップS12-1で受信パケットの送信元IPアドレスがフィルタ情報記憶部15に記憶されているかをパケット判断部23により判定し、記憶されてないと判定された場合は受信パケットがパケット判断部23によって廃棄される（ステップS12-2）。一方、パケットの送信元IPアドレスがフィルタ情報記憶部15に記憶されていると判定された場合は、受信パケットが通信の開始要求に関するものか否かがパケット判断部23によって判断される（ステップS12-3）。

[0040] ステップS12-3でパケットが通信の開始要求を表すものでないと判断された場合には、図4のステップS14に移り、受信パケットに対する暗号処理手順を実行する。一方、パケットが通信の開始要求を表すものであると判断された場合には、ステップS12-4でその受信パケットのヘッダに示されているIPアドレス、ポート番号などと対応するSA情報が暗号通信路情報記憶部12に記憶されているか否かが判断され、記憶されていなければステップS13-1でSA情報が暗号通信路情報合意部11によって相手装置3と合意される。

[0041] ステップS13-1で相手装置3と合意された情報は、ステップS13-2で暗号通信路情報記憶部12に記憶され、ステップS13-3で、フィルタ情報記憶部15に記憶されている送信元IPアドレスの端末装置5に関するフィルタ情報を参照して送信元の端末装置5が暗号処理機能を備えているか判定する。この判定は、例えば図2Bに示す送信元端末装置に関するフィルタ情報のプロトコルがtcpであり、かつ、処理指示がバイパスとなっている場合にその端末装置は暗号処理機能を備えていると判定する。暗号

処理機能を有していると判定した場合は、ステップS13-4でその合意したSA情報中の鍵情報を鍵情報設定部22によって端末インタフェイス14を介して送信元端末装置5に送信し、ステップS11に戻って次のパケットを受信する。

[0042] ステップS13-3で端末装置が暗号処理機能を備えてないと判定した場合は、そのままステップS11に戻って次のパケットを受信する。

ステップS12-4で有効なSA情報が記憶されていると判断されると、ステップS13-3に移り、前述と同様の処理を行う。なお、端末装置5は鍵情報設定部22により与えられた鍵情報が表す鍵を使って端末装置5と相手装置3との間で伝送されるパケットの暗号化及び復号化を行うが、端末装置5に鍵情報を送らない場合(すなわち端末装置が暗号処理機能を備えてない場合)は、端末装置と相手装置間で伝送されるパケットに対し、パケット暗号処理代理装置10が暗号化、復号化を代行する。

[0043] 以上で説明した、第1実施例及び第2実施例によるパケット暗号処理代理装置10の各構成要素は、上記で説明した動作をさせるように記述されたプログラムをプロセッサに実行させるようにしてもよい。即ち、復号化部13、端末情報収集部20、復号化判断部16、受信パケット判断部17、暗号化部18、及び暗号化判断部19、更に第2実施例の場合は、パケット判断部21,23を上記プログラムを実行するコンピュータによって構成するようにしてもよい。この場合、コンピュータ内にこのパケット暗号処理代理プログラムをCD－ROM、磁気ディスク、半導体記憶装置などの記録媒体からインストール又は通信回線を通じてダウンロードしてそのプログラムをコンピュータに実行させればよい。

[0044] また、暗号通信路情報記憶部12及びフィルタ情報記憶部15のうち少なくとも一方は、記憶した情報の少なくとも一部、例えば暗号鍵情報、利用者名などが予定された(許された)以外の利用者により変更されないように、ICカード、USB(Universal Serial Bus)キー、SD(Secure Digital)メモリカードなどの、耐タンパ性のある着脱可能なデバイスによって構成してもよい。

一方、暗号通信路情報記憶部12及びフィルタ情報記憶部15のうち少なくとも一方は、端末装置5の利用者がインターネット2を介して認証された利用者あるいはシステムの管理者であるならば、記憶した情報の少なくとも一部を変更できるようにしてもよ

い。つまり、例えばパケット暗号処理代理装置10には、アクセスのためのIPアドレスを割り当てておき、管理者は端末装置5からそのIPアドレスを用いてパケット暗号処理代理装置10をアクセスしそのフィルタ情報記憶部15に記憶するフィルタ情報に対する変更を行う。このパケット暗号処理代理装置10に割り当てられたIPアドレスは端末装置5と相手装置3との間のパケット通信には使用されない。

[0045] 上述のように、この発明のパケット暗号処理代理装置10はゲートウェイに設けられ、端末装置5に接続されている。このパケット暗号処理代理装置10はIP機能をもたないものであり、図3及び4で説明したように、受信したパケットを暗号処理するか否かの判断をして、暗号処理をする場合はパケット送信元及び送信先を変更することなく暗号処理を行って、そのパケットを送信先へ転送し、暗号処理を行わない場合はそのままパケットを送信先へ転送する。つまり暗号処理を行う場合と行わない場合とによりIPアドレスを変更したり、2つのIPアドレスを用いたりする必要がなく、従来のゲートウェイに設けられている、IP機能をもつパケット暗号処理代理装置とは異なる。

[0046] この発明のパケット暗号処理代理装置としてはフィルタ情報に基づく処理を行わなくてもよく、つまり単に暗号処理を行うだけでもよく、その場合も、暗号処理機能をもたない端末装置と相手装置とのパケット暗号通信の際に、相手装置はパケット送信先として端末装置のIPアドレスを付加すればよく、暗号処理代理装置のIPアドレスを用いる必要はない。

この発明のパケット暗号処理代理装置10はインターネット2と端末装置5との間に接続されていればよく、例えば図1に破線で示すようにLAN4と各端末装置5との間に接続してよい。この場合は端末装置5にはLANとの接続カード、つまりIP機能をもつ接続カードが装着されているからそのLAN接続カードにパケット暗号処理代理装置10を搭載してもよい。

[0047] IPSec機能はIP機能の一部として実装される。従って従来においてはゲートウェイのIP機能にIPSec機能が組み込まれ、あるいは端末装置のIP機能にIPSec機能が組み込まれていた。しかしこの発明の実施例のパケット暗号処理代理装置10ではIP機能に組み込まれることなく、最も簡単なものは暗号通信路情報記憶部12と暗号処理部（例えば復号化部13と暗号化部18）だけの機能を持っていればよく、つまりIP機能と

切り離され、送信先及び送信元を変更することなく単に暗号処理をして通過させるものである。従って単に端末装置のIPアドレスをパケットに設定すればよく端末装置のIPアドレスとパケット暗号処理代理装置のIPアドレスとの両アドレスをパケットに設定したり、IPアドレスの使い分けをする必要がなく、また暗号処理代行サーバのIPアドレスを入手した後にパケット暗号処理を行う繁雑さもない。

[0048] このようにこの発明の実施例のパケット暗号処理代理装置10はそのIPSec機能はIP機能に組み込まれるものでないから、インターネット2と端末装置5との間であればいずれの箇所に挿入してもよい。例えば図1又は5中に破線で示すようにLAN4と端末装置5との間に挿入してもよい。この場合は端末装置5に搭載されている、インターネットを介する通信機能、つまりIP機能が有線LANカードや無線LANカードなどのネットワークインタフェイスデバイスにこの実施例のパケット暗号処理代理装置10を実装してもよく、この発明の装置10は端末装置5に論理的に直接接続されてもよい。

[0049] 同様に図1又は2中に破線で示すようにLAN4に2ポートイーサネット(登録商標)ブリッジ6を介して端末装置5が接続されている場合のようにIPアドレスを持たないネットワーク間接続機器6にこの実施例のパケット暗号処理代理装置10を実装してもよい。つまりインターネットと端末装置5との間に接続されているIPアドレスを持たないデバイス6にこの発明による装置10を実装してもよい。更に図1又は5中に破線で示すように例えば家庭内のパーソナルコンピュータなどのIP機能をもつ端末装置5が公衆通信網7を介してインターネット2に接続されている場合に、その端末装置5と公衆通信網7との間にこの第1又は第2実施例のパケット暗号処理代理装置10を挿入してもよい。つまり端末装置5はインターネット2と論理的に直接接続されている場合でもこの実施例を適用することができる。

[0050] この発明において暗号処理とは前述したように、データを秘匿する、つまり暗号化する処理、その秘匿データとの秘匿を解除する、つまり復号化する処理、電子署名などデータの完全性を保証する処理、その電子署名の検証などの完全性を確認する処理のいずれかである。従って、図1及び5において、例えば復号化部13及び暗号化部18は暗号処理手段を構成するが、暗号処理手段は復号化、暗号化に限らず、電子署名の検証、電子署名の付加を行う手段であってもよい。同様に、暗号処理判

断手段として復号化判断部16及び暗号化判断部19が設けられているが、復号化、暗号化の判断に限らず、電子署名の検証を行うか否か、あるいは電子書名の添付を行うか否かの判断を行ってもよい。

[0051] 相手装置3から受信したパケットに対してのみこの発明を適用してもよく、逆に端末装置5から受信したパケットに対してのみこの発明を適用してもよい。例えば前者の場合は図1中の暗号化部18及び暗号化判断部19は省略され、端末インタフェイス14に受信されたパケットはそのままネットワークインタフェイス9に送られ、後者の場合は復号化判断部16、受信パケット判断部17、復号化部13が省略され、ネットワークインタフェイス9に受信されたパケットはそのまま端末インタフェイス14に送られる。図5の実施例では更に前者の場合はパケット判断部23が、後者の場合はパケット判断部21が省略される。

[0052] 図1及び5に示す構成中の受信パケット判断部17は省略してもよい。つまり受信パケットの正当性の判断は端末装置5のIP機能により判断させてもよい。しかし受信パケット判断部17を設ければ不必要なパケットに対し無駄な復号化処理がなされない効果がある。

フィルタ情報記憶部15及び復号化判断部16を省略してもよい。この場合は端末装置5に対し送信するパケットは全て暗号処理されたパケットにする必要がある。しかしこれらフィルタ情報記憶部15及び復号化判断部16を設ければ、パケットのデータに要求される事項などに応じて、暗号処理するかしないかを使い分けてパケットを端末装置5に送信することができ、暗号処理を施さなくてもよいパケットに対して暗号処理しないで済み、相手装置3の処理が簡単になる。フィルタ情報記憶部15及び暗号化判断部19も同様に省略することができる。しかしこれらフィルタ情報記憶部15及び暗号化判断部19を設ければ同様に不必要に暗号化処理を行わないで済み、このパケット暗号処理代理装置10の処理負荷が軽くなる。

[0053] なお暗号処理部と暗号通信路情報記憶部のみを設けたパケット暗号処理代理装置10を端末装置5の直前に設ける場合においても、利用者名や装置製造番号など外部に秘匿しておきたいデータに対し暗号化されるために有効である。 端末装置5は、例えば空調機、照明器具、洗濯機、電話機、電子レンジ、テレビジョン受像機、

パーソナルコンピュータなどの家庭内電気機器、事務用電気機器などその他あらゆる電気機器であって、IP機能を備えるものである。LAN4は無線LAN，有線LANでもよく、用途的に云えばホームネットワーク、企業内ネットワーク、学校内ネットワーク、地域ネットワーク、病院内ネットワークなどである。

[0054] 上述でパケットに対する暗号処理をIPSecにより準拠して行ったが、他の規格SSL(Secure Sockets Layer)やTLS(Transport Layer Security) などにより暗号処理を行ってもよい。

請求の範囲

[1] インターネットと端末装置との間に接続された装置であって、

インターネットに接続された相手装置と前記端末装置との間のパケット通信における少なくともインターネット上のパケット通信に対し、暗号通信路の確立に用いる暗号通信路情報を記憶する暗号通信路情報記憶部と、

受信されたパケットに対して暗号処理を上記暗号通信路情報記憶部に記憶されている暗号通信路情報に基づいて行う暗号処理手段、

とを含むパケット暗号処理代理装置。

[2] 請求項1記載のパケット暗号処理代理装置は、さらに送信元識別情報、送信先識別情報、パケット通信手順を表すプロトコル情報及び暗号処理をするか否かを示す処理指示情報をフィルタ情報として記憶するフィルタ情報記憶部と、

このパケット暗号処理装置に受信されたパケット中のフィルタ情報により前記フィルタ情報記憶部を参照してその処理指示情報に基づき前記受信されたパケットを前記暗号処理手段によって暗号処理をするか否かを判断する暗号処理判断手段を含む。

[3] 請求項1記載のパケット暗号処理代理装置は、さらに前記相手装置から受信されたパケットが正当なものであるか否かを判断する受信パケット判断部を含む。

[4] 請求項1記載のパケット暗号処理代理装置において、前記暗号通信路情報記憶部は、前記暗号通信路情報中の少なくとも一部が記憶された、着脱可能な耐タンパ性デバイスを含む。

[5] 請求項1記載のパケット暗号処理代理装置において、前記暗号通信路情報記憶部は前記暗号通信路情報中の少なくとも一部が変更可能な記憶媒体を含む。

[6] 請求項1乃至5のいずれか記載のパケット暗号処理代理装置は、前記端末装置のネットワークインタフェイスデバイスに論理的に直接接続されている。

[7] 請求項1乃至5のいずれか記載のパケット暗号処理代理装置は、前記インターネットと前記端末装置との間に接続されたIPアドレスを持たないデバイスに実装されている。

[8] 請求項2乃至5のいずれか記載のパケット暗号処理代理装置は、さらに前記暗号

通信路情報及び前記フィルタ情報の少なくとも一方の一部の情報を前記端末装置から収集し、前記フィルタ情報記憶部に記憶する端末情報収集部を含む。

[9] 請求項1記載のパケット暗号処理代理装置は、さらに

前期相手装置と前記端末装置との間のパケット通信路を確立するための暗号通信路情報を前記相手装置と合意する必要があるか否かを、受信されたパケットから判断するパケット判断部と、

前記パケット判断部が合意を必要とすると判断すると前記合意を行い、前記暗号通信路情報記憶部に合意された暗号通信路情報を記憶する暗号通信路情報合意部と、

前記暗号通信路情報合意部によって合意された暗号通信路情報中の、パケットを暗号処理するための鍵情報を前記端末装置に設定する鍵情報設定部、

とを含む。

[10] 請求項9記載のパケット暗号処理代理装置において、前記パケット判断部は、暗号通信路情報の合意を必要とすると判断すると前記受信パケットと対応する有効な暗号通信路情報が前記暗号通信路情報記憶部に記憶されているかを判断し、記憶されていればその暗号通信路情報中の鍵情報を前記鍵情報設定部により前記端末装置に設定させ、記憶されてなければ前記暗号通信路情報合意部に暗号通信路情報の合意を実行させる。

[11] 請求項10記載のパケット暗号処理代理装置において、前記パケット判断部は、前記暗号通信路情報の合意を必要とすると判断し、かつ前記受信されたパケット内のアドレス情報が前記フィルタ情報記憶部に記憶されていれば前記鍵情報の合意を実行させる。

[12] 請求項11記載のパケット暗号処理代理装置はさらに、前記端末装置を検知して、その端末装置からアドレス情報を取得し、その取得したアドレス情報を前記フィルタ情報記憶部に記憶する端末情報取得部を含んでいる。

[13] (a) インターネットに接続された相手装置と端末装置の間のパケット通信における少なくともインターネット上のパケット通信に対し、暗号通信路の確立に用いる暗号通信路情報を前記相手装置と合意して暗号通信路情報記憶部に記憶する工程と、

(b) 前記暗号通信路情報に基づいて、受信されたパケットに対し暗号処理を行う工程、

とを含むパケット暗号処理方法。

[14] 請求項13記載のパケット暗号処理方法において、前記工程(b)は、

(b-1) 前記受信されたパケット中のフィルタ情報により、フィルタ情報記憶部を参照して前記受信されたパケットに対し、暗号処理をするか、否かを判断する工程と、

(b-2) 前記判断が暗号処理すると判断した場合は、前記暗号処理を実行させ、前記判断が暗号処理しないと判断した場合は、前記受信されたパケットをそのまま通過又は廃棄する工程とを含む。

[15] 請求項13記載のパケット暗号処理方法において、前記工程(a)は、

(a-1) 受信されたパケットが暗号通信路情報の合意を必要とするか否かを判断し、合意が必要であればインターネットに接続された相手装置と端末装置との間のパケット通信に対し、前記相手装置との間で伝送されるパケットを暗号処理する暗号通信路情報を前記相手装置と合意する工程と、

(a-2) 合意された暗号通信路情報を前記端末装置に設定する工程と、

(a-3) 合意が必要でないならば前記受信されたパケットをバイパス又は廃棄する工程、

とを含む。

[16] 請求項15記載のパケット暗号処理方法において、前記工程(a-1)は、

(a-1-1) 前記受信パケットに対する暗号通信路情報の合意が必要であれば、前記受信パケットと対応する有効な暗号通信路情報が前記暗号通信路情報記憶手段に記憶されているかを判断する工程と、

(a-1-2) 暗号通信路情報が記憶されているならばその暗号通信路情報中の鍵情報を前記端末装置に設定し、暗号通信路情報が記憶されてないならば前記暗号通信路情報の合意を実行し、合意した暗号通信情報を暗号通信路情報記憶部に記憶し、かつ前記端末装置に設定する工程、

とを含む。

[17] 請求項16記載のパケット暗号処理方法において、前記工程(a-1-1)は前記パケッ

トに対する暗号通信路情報の合意が必要であれば、まず前記受信パケット内のアドレス情報がフィルタ情報記憶部に記憶されているかを判断し、記憶されてれば、前記暗号通信路情報記憶部に有効な暗号通信路情報が記憶されているかの前記判断を行う工程を含む。

[18] 請求項13～17のいずれかに記載したパケット暗号処理方法をコンピュータで実行するプログラムが記録された読み取り可能な記録媒体。

[図1]

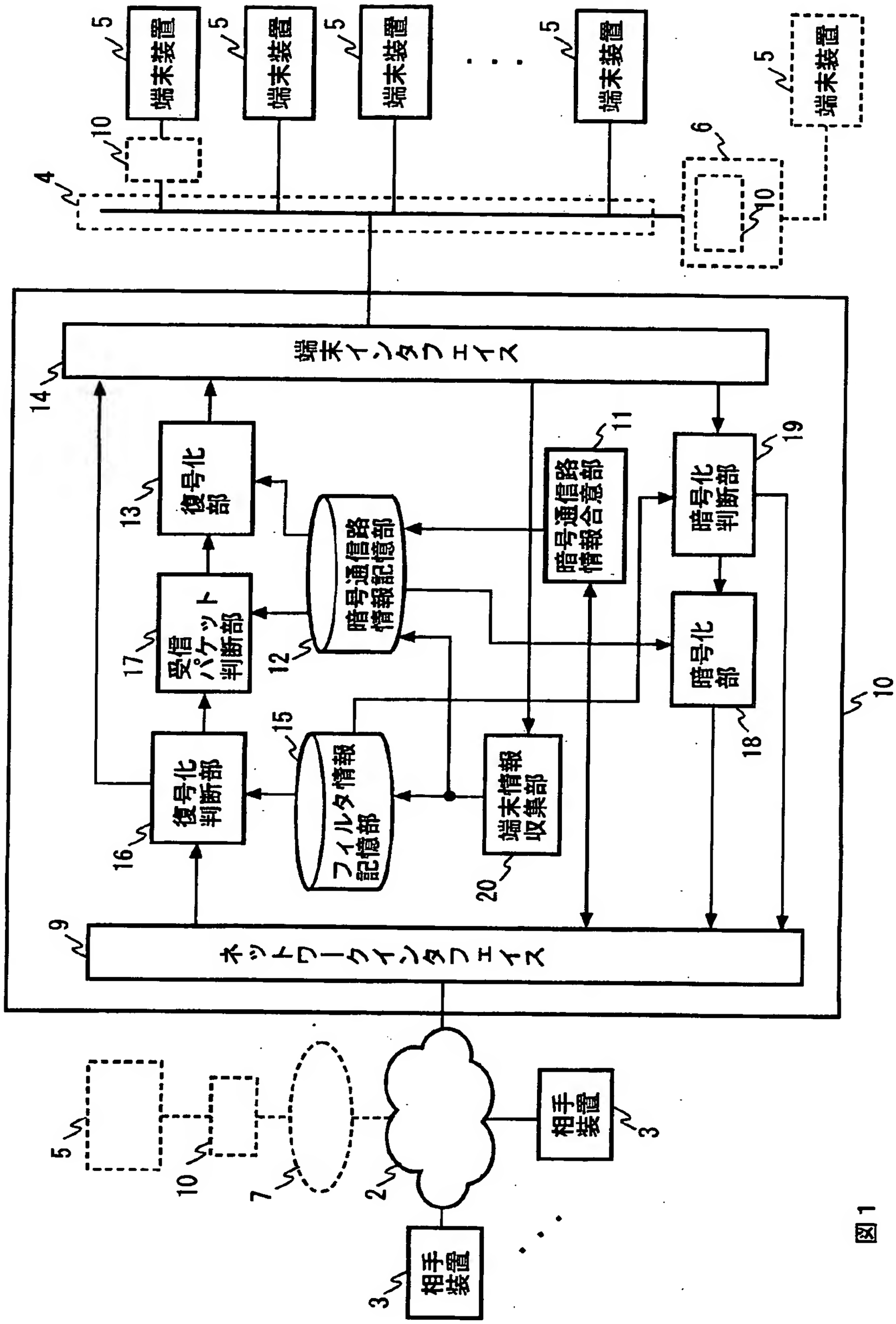

端末装置
5
10
4
6
端末インタフェース
14
復号化部
13
暗号通信路情報記憶部
12
暗号通信路情報合意部
11
暗号化判断部
19
受信パケット判断部
17
暗号化部
18
復号化判断部
16
フィルタ情報記憶部
15
端末情報収集部
20
ネットワークインタフェース
9
10
7
2
3

図1

図２Ａ

ＳＡ情報

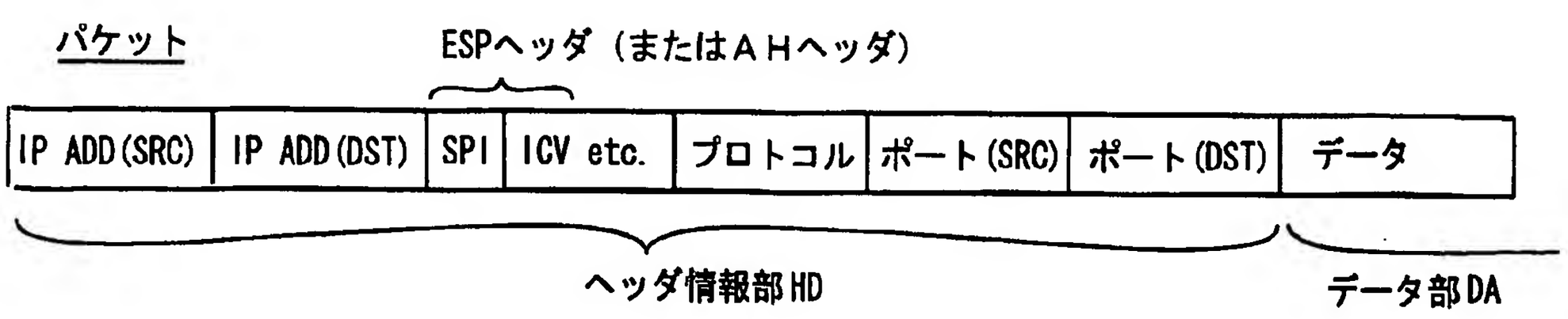
端末ＩＰアドレス	ＳＰＩ	プロトコル	暗号アルゴリズム、鍵	モード	相手ＩＰアドレス	存続期間

図２Ｂ

フィルタ情報

送信元ＩＰアドレス	送信先ＩＰアドレス	プロトコル	送信元ポート番号	送信先ポート番号	処理指示
10.0.0.1/32	10.0.0.*/24	tcp	any	any	暗号処理
10.0.0.2/32	10.0.1.*/24	IPSec	N/A	N/A	バイパス
2001::1	2001::2	udp	137	137	バイパス
2001::1/128	2001::2/128	icmp	135	N/A	廃棄

図２Ｃ



[図3]

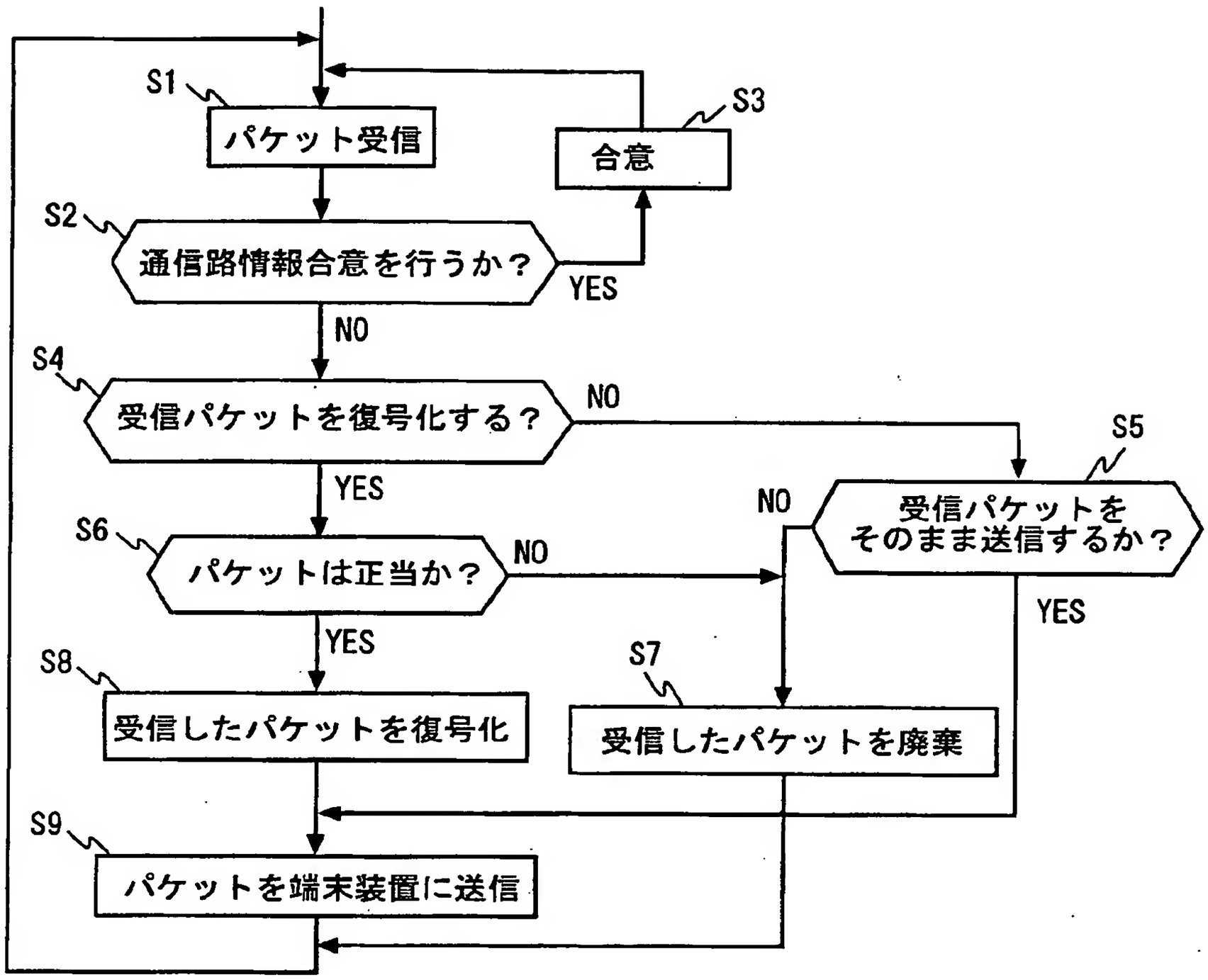

S1
パケット受信
S2
通信路情報合意を行うか？
YES
S3
合意
NO
S4
受信パケットを復号化する？
NO
S5
受信パケットを
そのまま送信するか？
YES
NO
S6
パケットは正当か？
NO
YES
S7
受信したパケットを廃棄
S8
受信したパケットを復号化
S9
パケットを端末装置に送信

図3

[図4]

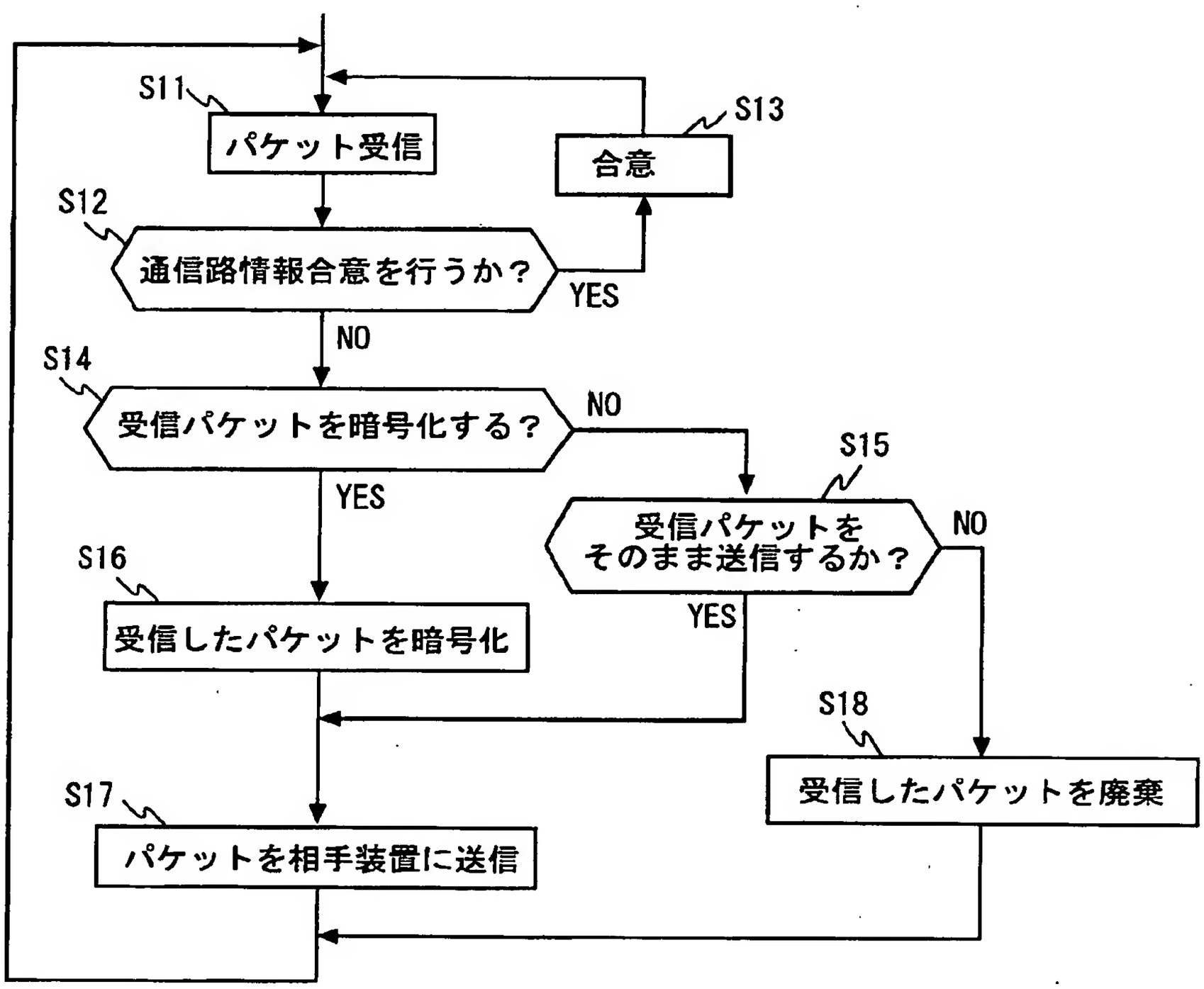

S11
パケット受信
S12
通信路情報合意を行うか？
YES
S13
合意
NO
S14
受信パケットを暗号化する？
NO
S15
受信パケットを
そのまま送信するか？
NO
YES
S16
受信したパケットを暗号化
YES
S17
パケットを相手装置に送信
S18
受信したパケットを廃棄

図４

[図5]

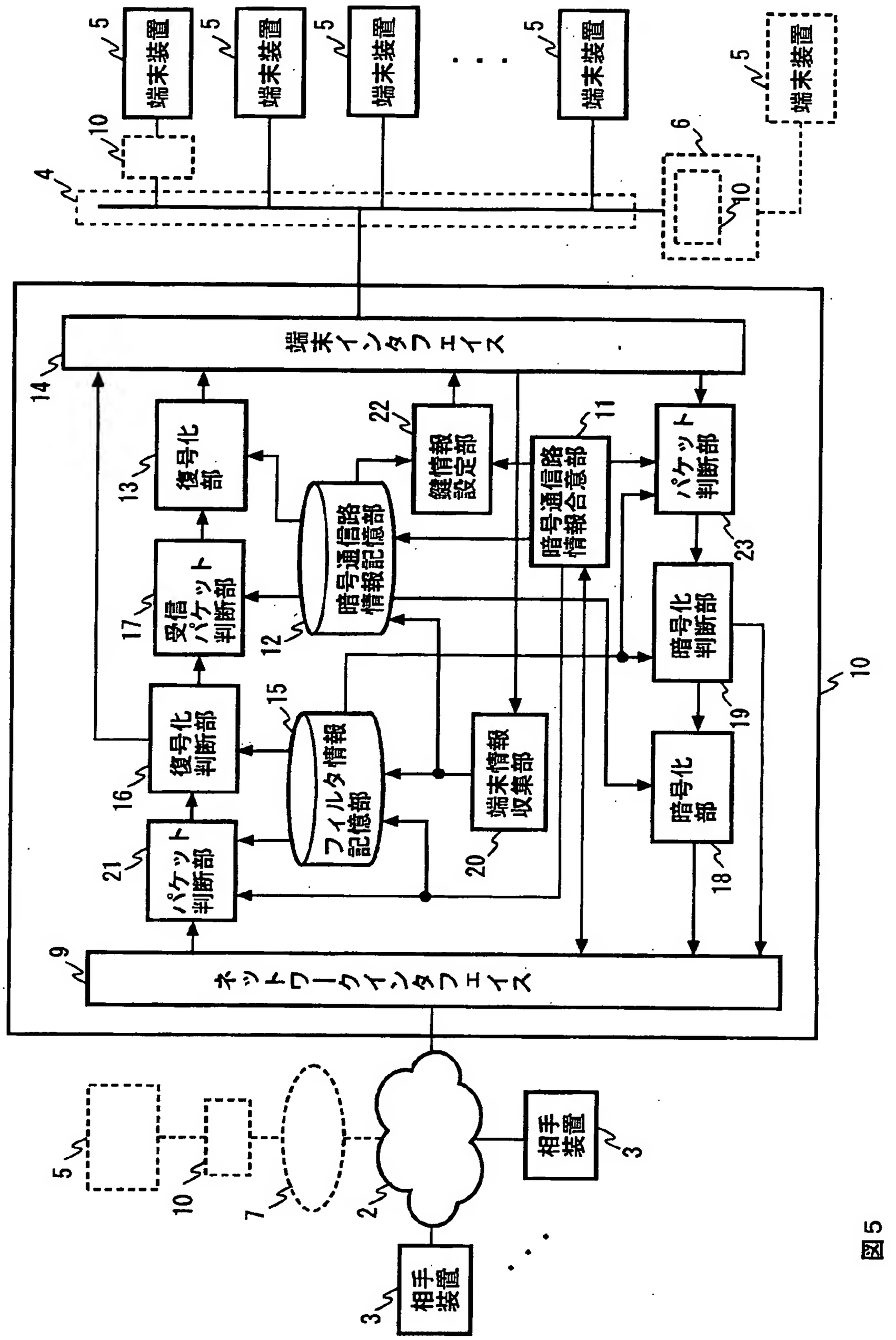

端末装置
端末装置
端末装置
端末装置
端末装置
10
4
6
10
端末インタフェース
14
復号化部
13
鍵情報設定部
22
暗号通信路情報合意部
11
パケット判断部
23
受信パケット判断部
17
暗号通信路情報記憶部
12
暗号化判断部
復号化判断部
16
フィルタ情報記憶部
15
端末情報収集部
20
暗号化部
パケット判断部
21
19
18
ネットワークインタフェース
9
10
5
10
7
2
相手装置
3
相手装置
3

図5

[図6]

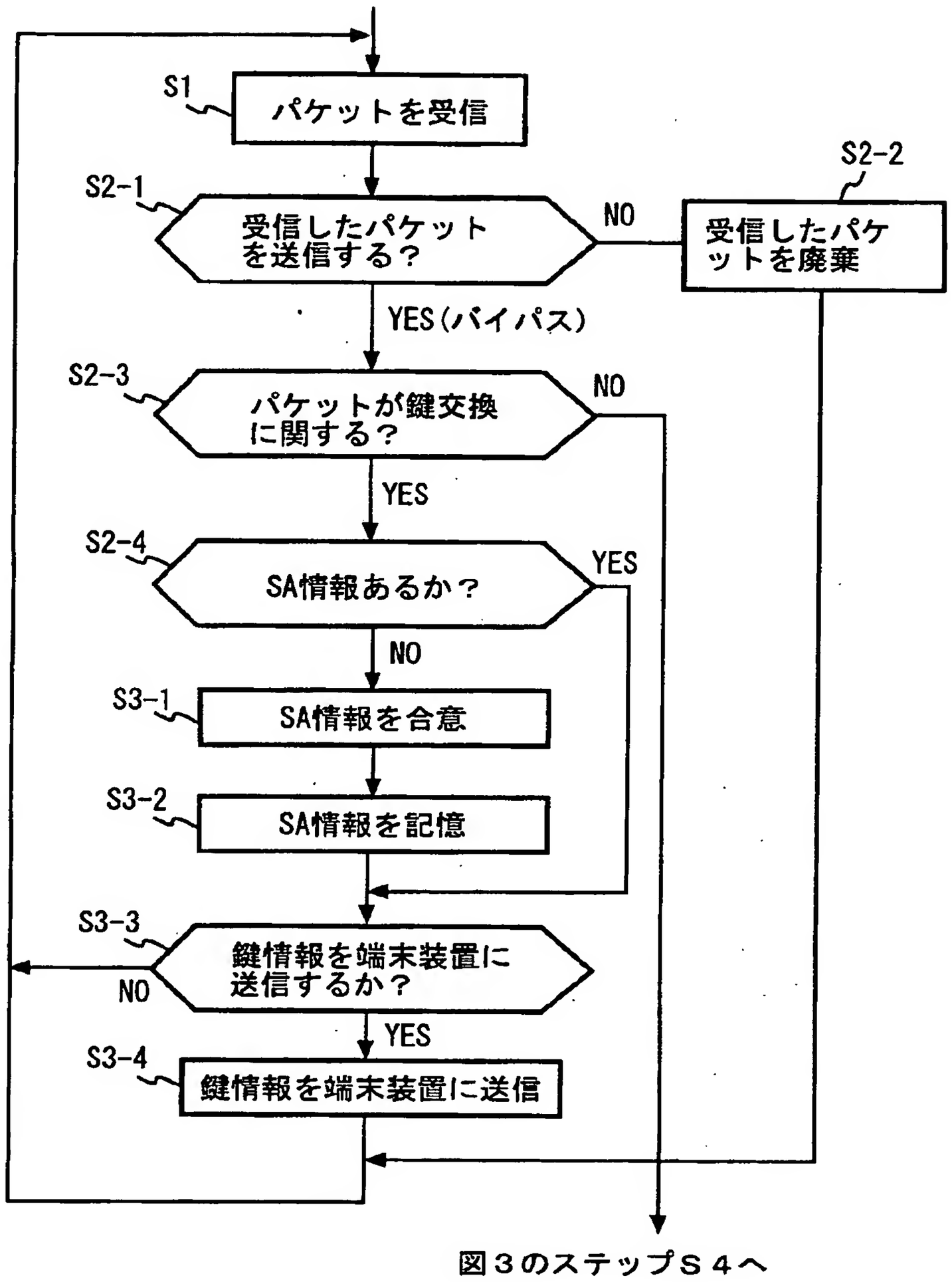

S1
パケットを受信
S2-1
受信したパケットを送信する？
NO
S2-2
受信したパケットを廃棄
YES(バイパス)
S2-3
パケットが鍵交換に関する？
NO
YES
S2-4
SA情報あるか？
YES
NO
S3-1
SA情報を合意
S3-2
SA情報を記憶
S3-3
鍵情報を端末装置に送信するか？
NO
YES
S3-4
鍵情報を端末装置に送信
図３のステップＳ４へ

図６

[図7]

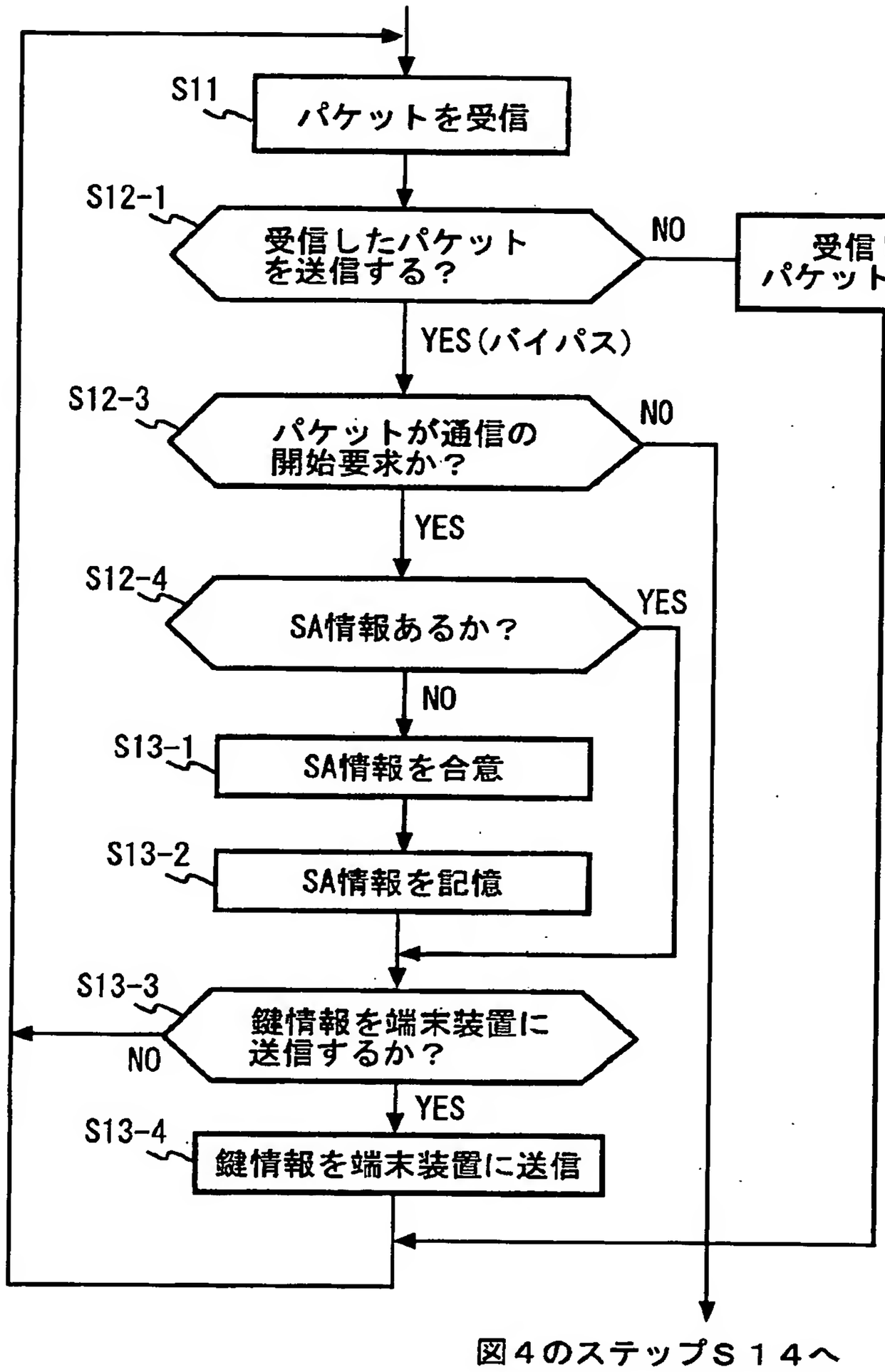

S11
パケットを受信
S12-1
受信したパケット
を送信する？
NO
S12-2
受信した
パケットを廃棄
YES(バイパス)
S12-3
パケットが通信の
開始要求か？
NO
YES
S12-4
SA情報あるか？
YES
NO
S13-1
SA情報を合意
S13-2
SA情報を記憶
S13-3
鍵情報を端末装置に
送信するか？
NO
YES
S13-4
鍵情報を端末装置に送信
図４のステップＳ１４へ

図７

[図8]

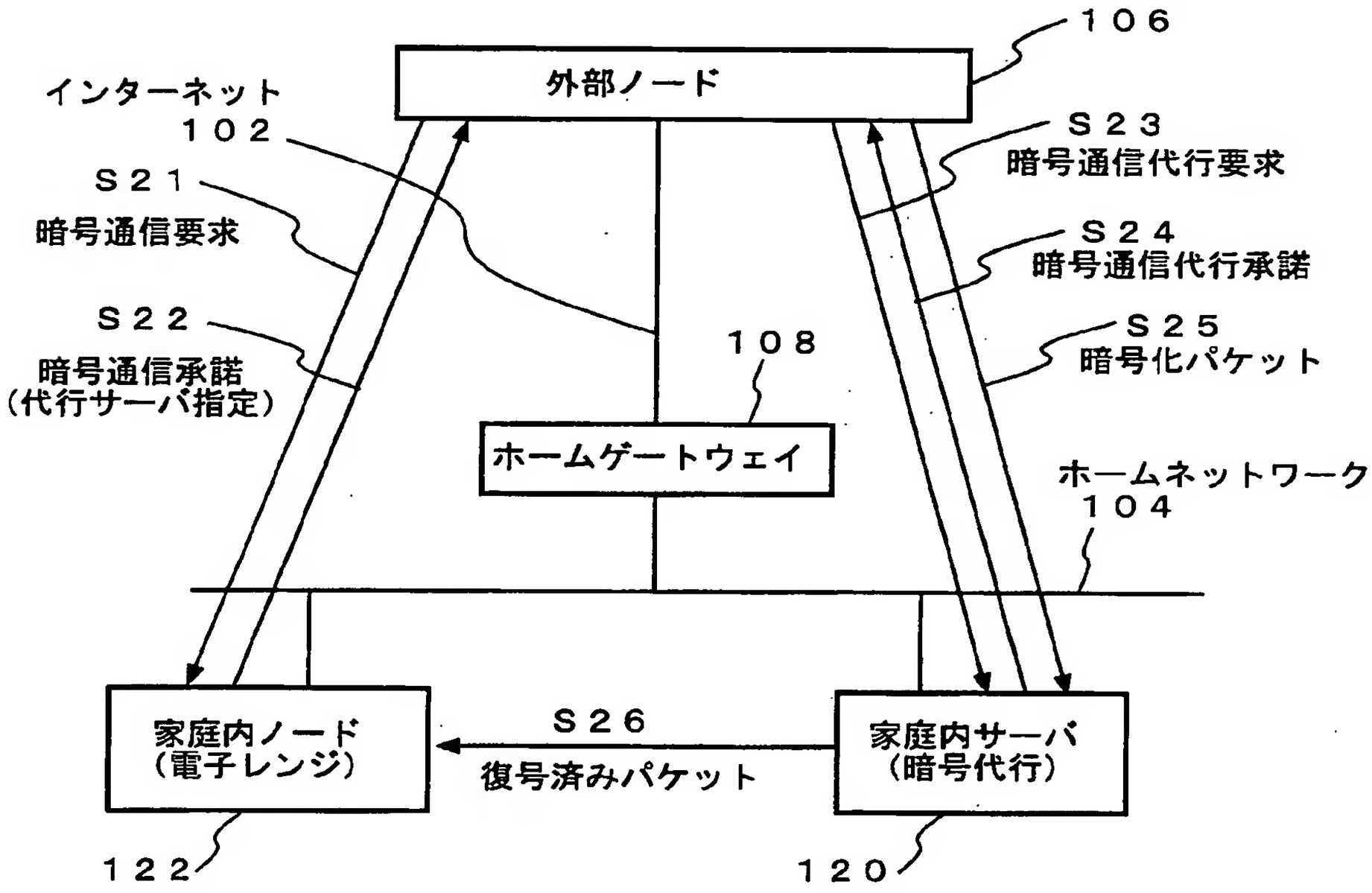

インターネット
102
S21
暗号通信要求
S22
暗号通信承諾
(代行サーバ指定)
外部ノード
106
S23
暗号通信代行要求
S24
暗号通信代行承諾
S25
暗号化パケット
108
ホームゲートウェイ
ホームネットワーク
104
家庭内ノード
(電子レンジ)
S26
復号済みパケット
家庭内サーバ
(暗号代行)
122
120

図8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/006624

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/36

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/36, H04L12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2005
Kokai Jitsuyo Shinan Koho	1971-2005	Toroku Jitsuyo Shinan Koho	1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2003-179627 A (Mitsubishi Electric Corp.), 27 June, 2003 (27.06.03), Figs. 1 to 4 (Family: none)	1-7,13,14 8-12,15-18
Y	JP 11-308264 A (Mitsubishi Electric Corp.), 05 November, 1999 (05.11.99), Par. Nos. [0006] to [0009] (Family: none)	8,12
Y	2001-7849 A (Toshiba Corp.), 12 January, 2001 (12.01.01), Figs. 18, 19 (Family: none)	9-11,15-18

[×] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 17 May, 2005 (17.05.05)	Date of mailing of the international search report 31 May, 2005 (31.05.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/006624

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-69597 A (NEC Corp.), 07 March, 2003 (07.03.03), Figs. 2, 4, 6 (Family: none)	9-11,15-18
X	JP 2003-110628 A (NEC Corp.), 11 April, 2003 (11.04.03), Figs. 1 to 7 (Family: none)	1,13,14
A	JP 6-37750 A (Hitachi, Ltd.), 10 February, 1994 (10.02.94), Figs. 6 to 11 (Family: none)	1-18

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００６６２４

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L9/36

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　H04L9/36 , H04L12/66

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X Y	ＪＰ ２００３－１７９６２７ Ａ（三菱電機株式会社） ２００３.０６.２７，第１－４図　（ファミリーなし）	1-7, 13, 14 8-12, 15-18
Y	ＪＰ １１－３０８２６４ Ａ（三菱電機株式会社） １９９９.１１.０５，【０００６】－【０００９】段落 （ファミリーなし）	8, 12

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 １７．０５．２００５	国際調査報告の発送日 31.5.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９４６９ 石田　信行 電話番号　０３－３５８１－１１０１　内線　３５４６

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ２００５／００６６２４

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	２００１－７８４９　Ａ（株式会社東芝） ２００１．０１．１２，第１８，１９図　（ファミリーなし）	9-11, 15-18
Ｙ	ＪＰ　２００３－６９５９７　Ａ（日本電気株式会社） ２００３．０３．０７，第２，４，６図　（ファミリーなし）	9-11, 15-18
Ｘ	ＪＰ　２００３－１１０６２８　Ａ（日本電気株式会社） ２００３．０４．１１，第１－７図　（ファミリーなし）	1, 13, 14
Ａ	ＪＰ　６－３７７５０　Ａ（株式会社日立製作所） １９９４．０２．１０，第６－１１図　（ファミリーなし）	1-18